

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

In re Patent Application of:)
HYLAND)
)
Serial No.: 10/806,936) Attorney Docket No.:
) GCSD-1576 (51398)
Confirmation No: 2856)
)
Filing Date: MARCH 23, 2004)
)
For: MODULAR CRYPTOGRAPHIC DEVICE)
AND COUPLING THEREFOR AND)
RELATED METHODS)
)
)

APPELLANT'S AMENDED APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Responsive to the Notification of Non-Compliant Appeal Brief mailed November 18, 2009, submitted herewith is Appellant's Amended Appeal Brief. If any additional extension and/or fee is required, authorization is given to charge Deposit Account No. 08-0870.

(1) Real Party in Interest

The real party in interest is Harris Corporation, assignee of the present application as recorded at reel 015516, frame 0053.

(2) Related Appeals and Interferences

At present there are no related appeals or interferences.

In Re Patent Application of:

HYLAND

Serial No. **10/806,936**

Filing Date: **MARCH 23, 2004**

/

(3) Status of the Claims

Claims 1, 4-12, 14-21, 24-28 and 31-38 are pending in the application. Claims 2, 3, 13, 22, 23, 29, and 30 have been cancelled. The Examiner's rejection of Claims 1, 4-12, 14-21, 24-28 and 31-38 is being appealed herein.

(4) Status of the Amendments

All amendments have been entered and there are no further pending amendments. A copy of the claims involved in this appeal is attached hereto as Appendix A.

(5) Summary of the Claimed Subject Matter

Independent Claim 1 recites a cryptographic device comprising a cryptographic module and a communications module removably coupled thereto (paragraph 30, figs 12-14). The cryptographic module comprises a first housing and a first connector carried thereby, the first housing comprising a first body and a first extension extending outwardly therefrom (paragraphs 34, 71, 72, figs 12-14). The communications module comprises a second housing and a second connector carried thereby and being removably mateable with the first connector of the cryptographic module (paragraphs 37, 71, 72, figs 12-14). The second housing comprises a second body and a second extension extending outwardly therefrom (paragraphs 37, 71, 72, figs 12-14). The first and second extensions are aligned in overlapping relation when the first and second connectors are mated together (paragraphs 71, 72, figs 12-14). The first connector is carried by the first body adjacent the first extension and the second connector is carried by the second extension (paragraphs 71, 72, figs 12-14).

Dependent Claim 4 recites that each of the first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules together in mating relation (paragraph 73, figs 12-14).

Dependent Claim 5 recites that the surface features define at least one slidable interlocking joint therebetween (paragraph 73, figs 12-14).

Dependent Claim 6 recites at least one fastener for removably fastening the cryptographic and communications modules together (paragraph 73, figs 12-14).

Dependent Claim 7 recites that the at least one fastener comprises at least one captive screw (paragraph 73, figs 12-14).

Dependent Claim 8 recites that the communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (paragraph 68).

Dependent Claim 9 recites that the communications module further comprises a network communications interface carried by the second housing and coupled to the second connector (paragraph 37, fig 4).

Dependent Claim 10 recites that the first and second connectors each comprise multi-pin electrical connectors (paragraph 74, figs 12-14).

Dependent Claim 11 recites at least one seal between the cryptographic module and the communications module (paragraph 74, figs 12-14).

Independent Claim 12 recites a cryptographic device comprising a cryptographic module, a communications module removably coupled to the cryptographic module, and at least one

fastener for removably fastening the cryptographic and communications modules together (paragraphs 30, 74, figs 12-14). The cryptographic module comprises a first housing and a first connector carried thereby, the first housing comprising a first body and a first extension extending outwardly therefrom (paragraphs 34, 71, 72, figs 12-14). The communications module comprises a second housing and a second connector carried thereby, the second housing comprising a second body and a second extension extending outwardly therefrom (paragraphs 34, 71, 72, figs 12-14). The second connector is removably mateable with the first connector of the cryptographic module, and the first and second extensions are aligned in overlapping relation when the first and second connectors are mated together (paragraphs 34, 71, 72, figs 12-14). The first connector is carried by the first body adjacent the first extension and the second connector is carried by the second extension (paragraphs 34, 71, 72, figs 12-14).

Dependent Claim 14 recites that each of the first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules together in mating relation (paragraph 73, figs 12-14).

Dependent Claim 15 recites that the surface features define at least one slidably interlocking joint therebetween (paragraph 73, figs 12-14).

Dependent Claim 16 recites that the at least one fastener comprises at least one captive screw (paragraph 73, figs 12-14).

Dependent Claim 17 recites that the communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating

over a different communications media (paragraph 68).

Dependent Claim 18 recites that the communications module further comprises a network communications interface carried by the second housing and coupled to the second connector (paragraph 37, fig 4).

Dependent Claim 19 recites that the first and second connectors each comprise multi-pin electrical connectors (paragraph 74, figs 12-14).

Dependent Claim 20 recites at least one seal between the cryptographic module and the communications module (paragraph 74, figs 12-14).

Independent Claim 21 recites a communications method comprising coupling a cryptographic module to a network device, the cryptographic module comprising a first housing and a first connector carried thereby, the first housing comprising a first body and a first extension extending outwardly therefrom (paragraphs 30, 34, 71, 72, figs 12-14). The method also includes providing a communications module comprising a second housing and a second connector carried thereby with the second connector of the communications module being removably mated with the first connector of the cryptographic module, the second housing comprising a second body and a second extension extending outwardly therefrom (paragraphs 34, 71, 72, figs 12-14). The first and second extensions are aligned in overlapping relation when the first and second connections are mated together, the first connector carried by the first body adjacent the first extension and the second connector carried by the second extension (paragraphs 34, 71, 72, figs 12-14). The method further includes using the communications module to communicate with a network (paragraph 30).

Dependent Claim 24 recites that each of the first and

second extensions have surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules together in mating relation (paragraph 73, figs 12-14).

Dependent Claim 25 recites that the surface features define at least one slidable interlocking joint therebetween (paragraph 73, figs 12-14).

Dependent Claim 26 recites removably fastening the cryptographic and communications modules together (paragraph 73, figs 12-14).

Dependent Claim 27 recites positioning at least one seal between the cryptographic module and the communications module (paragraph 74, figs 12-14).

Independent Claim 28 recites a communications system comprising a plurality of network devices coupled together to define a network, and a cryptographic device coupled to at least one of the network devices (paragraph 30, figs 1, 12-14). The cryptographic device comprises a cryptographic module coupled to the at least one network device, and a communications module removably coupled to the cryptographic module (paragraph 30, figs 12-14). The cryptographic module comprises a first housing and a first connector carried thereby, the first housing comprising a first body and a first extension extending outwardly therefrom (paragraphs 34, 71, 72, figs 12-14). The communications module comprises a second housing and a second connector carried thereby and being removably mateable with the first connector of the cryptographic module, the second housing comprising a second body and a second extension extending outwardly therefrom (paragraphs 34, 71, 72, figs 12-14). The first and second extensions are aligned in overlapping relation when the first and second connectors are mated together (paragraphs 71, 72, figs 12-14).

The first connector is carried by the first body adjacent the first extension and the second connector carried by the second extension (paragraphs 71, 72, figs 12-14).

Dependent Claim 31 recites that each of the first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules together in mating relation (paragraph 73, figs 12-14).

Dependent Claim 32 recites that the surface features define at least one slidable interlocking joint therebetween (paragraph 73, figs 12-14).

Dependent Claim 33 recites at least one fastener for removably fastening the cryptographic and communications modules together (paragraph 73, figs 12-14).

Dependent Claim 34 recites that the at least one fastener comprises at least one captive screw (paragraph 73, figs 12-14).

Dependent Claim 35 recites that the cryptographic module further comprises a user network interface carried by the first housing, and a cryptographic processor carried by the first housing and coupled to the user network interface and the first connector (paragraph 37, fig 4).

Dependent Claim 36 recites a network communications interface carried by the second housing and coupled to the second connector (paragraph 37, fig 4).

Dependent Claim 37 recites that the first and second connectors each comprise multi-pin electrical connectors (paragraph 74, figs 12-14).

Dependent Claim 38 recites at least one seal between the cryptographic module and the communications module (paragraph 74, figs 12-14).

In Re Patent Application of:

HYLAND

Serial No. **10/806,936**

Filing Date: **MARCH 23, 2004**

/

(6) *Grounds of Rejection to be Reviewed On Appeal*

Claims 1, 4-6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 24-28, 31-33, 35, 36 and 38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Dumont (EP 0891 112) in view of Janky (US 5,786,789). Claims 7, 10, 16, 19, 34, and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Dumont (EP 0891 112) in view of Janky (US 5,786,789) and further in view of Chou (US 2002/0111189).

(7) *Argument*

A. Claims 1, 12, 21, and 28 Are Patentable Over Dumont In View of Janky

Independent Claims 1, 12, 21, and 28 remain rejected over the combination of Dumont and Janky. Dumont discloses a communications system including a portable telephone and a transmission securing auxiliary module. The portable telephone comprises a housing and a female connector carried thereby. The transmission securing auxiliary module comprises a housing and a male connector carried thereby. The Examiner correctly recognized that Dumont fails to disclose that the second connector is carried by the second extension, as recited in independent Claims 1, 12, 21, and 28. In an attempt to provide this critical deficiency of Dumont, the Examiner looked to Janky.

Janky discloses a GPS unit to mate with a cellular telephone unit. The GPS unit and the cellular telephone unit each comprises a body and an extension extending outwardly therefrom. These extensions overlap each other.

Even this selective combination of Dumont and Janky, however, fails to disclose that the second connector is carried

by the second extension. The Examiner relied on Janky to provide this feature to the combination, yet Janky makes no such disclosure. In particular, the Examiner has taken the position that col. 2, lines 14-15, col. 5, lines 38-39, and FIGs. 4A-4B of Janky disclose this claimed feature. Applicant respectfully disagrees with the Examiner. These cited portions do not disclose a second connector carried by a second extension.

As stated by the Examiner on page 2 of the Official Action dated 4/27/2009, "Janky doesn't explicitly show the physical connectors." Yet, the Examiner somehow asserts that Janky shows precisely that. While col. 2, lines 14-15 of Janky recite that "the removable add-on module is removably coupled to the core module," they are silent as to how the removable add-on module and the core module are physically connected together. While FIGS. 4A and 4B show the removable add-on module and the core module physically coupled together, they fail to show any removably mateable connectors carried by either the removable add-on module or the core module.

Further, while FIGS. 5, 6, and 9 of Janky show that its removable add-on module and core module are electrically coupled so that signals may pass between the units, they are silent as to how this is accomplished as no connectors of either the GPS unit or the cellular telephone unit are shown. Likewise, no portion of Janky's specification discloses any such connector carried by either the extension of either the removable add-on module or the core module.

As such, Janky simply fails to disclose that the second connector is carried by the second extension, as recited in independent Claims 1, 12, 21, and 28. Dumont fails to provide this critical deficiency to the combination. Consequently, independent Claims 1, 12, 21 and 28 are patentable over the

In Re Patent Application of:
HYLAND
Serial No. 10/806,936
Filing Date: MARCH 23, 2004

combination of Janky and Dumont.

B. Claims 4, 14, 24, and 32 Are Patentable Over Dumont In View of Janky

The Examiner rejected dependent Claims 4, 14, 24, and 34 over the combination of Dumont and Janky. Dependent Claim 4, for example, recites that each of the first and second extensions has surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules together in mating relation. The Examiner asserted FIGS. 3A, 3B, 4A, 7B, and 8 of Janky to show these features.

The cited figures show no surface features of the removable add-on module and core module whatsoever. In fact, FIGS. 7B and 8 are block diagrams and provide no details beyond the fact that the removable add-on module and the core module somehow fit together. While FIGS. 3A, 3B, and 4B show some features of the core module and the removable add-on module, they show absolutely no surface details of the portions of each that the Examiner asserts to disclose the first and second extensions of dependent Claims 4.

As such, dependent Claim 4, and dependent Claims 14, 24, and 34, which contain similar recitations, are patentable over the combination of Dumont and Janky.

C. Claims 8 and 17 Are Patentable Over Dumont In View of Janky

The Examiner rejected dependent Claims 8 and 17 over the combination of Dumont and Janky. Dependent Claims 8 and 17 recite that the communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media. The Examiner asserted page 3, lines 17-20 of Dumont to

disclose these features. Page, lines 17-20 provide that:

Consequently, the user can add, as he chooses, an additional function to his standard portable telephone, simply by mounting this auxiliary module on the standard casing of the telephone.

Advantageously, some means arranged for being connected in parallel on the radio interface circuit of the portable telephone are provided.

Rather than disclosing that the portable telephone of Dumont (asserted to be the communications module of dependent Claims 8 and 17) comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media, this cited portion simply states that the singular auxiliary module (asserted to be the cryptographic module of dependent Claims 8 and 17) which is never described to be one from among a plurality of auxiliary modules, may be added to the portable telephone.

Indeed, it is clear that Dumont fails to teach or fairly suggest a plurality of interchangeable communications modules each for communicating over a different communications media. Indeed, Dumont merely discloses a portable telephone operating over a typical cellular band.

As such, Dumont, and therefore the combination of Dumont and Janky, fails to disclose a communications module comprising a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media, as recited in dependent Claims 8 and 17. Consequently, dependent Claims 8 and 17 are patentable over the combination of Dumont and Janky.

D. Claims 5-6, 9,11; 15, 18, 20; 25-27; and 32-33, 35-36, 38 Are

In Re Patent Application of:

HYLAND

Serial No. 10/806,936

Filing Date: MARCH 23, 2004

/

Patentable Over Dumont In View of Janky

The Examiner rejected dependent Claims 5-6, 9,11; 15, 18, 20; 25-27; and 32-33, 35-36, 38 over the combination of Dumont and Janky. As explained in detail above, Janky fails to disclose a second connector carried by a second extension, as recited in independent Claims 1, 12, 21, and 28, from which Claims 5-6, 9,11; 15, 18, 20; 25-27; and 32-33, 35-36, 38 depend upon, respectively. Dumont fails to provide this critical deficiency to the combination. Consequently, dependent Claims 5-6, 9,11; 15, 18, 20; 25-27; and 32-33, 35-36, 38 are patentable over the combination of Dumont and Janky.

E. Claims 7, 10, 16, 19, 34, and 37 Are Patentable Over Dumont In View of Janky In Further View of Chou.

The Examiner rejected dependent Claims 7, 10, 16, 19, 34, and 37 over the combination of Dumont, Janky, and Chou. As explained in detail above, Janky fails to disclose a second connector carried by a second extension, as recited in independent Claims 1, 12, and 28, from which Claims 7, 10, 16, 19, 34, and 37 depend upon, respectively. Dumont and Chou fail to provide this critical deficiency to the combination.

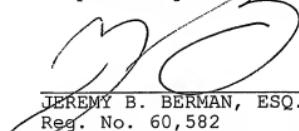
Consequently, dependent Claims 7, 10, 16, 19, 34, and 37 are patentable over the combination of Dumont, Janky, and Chou.

In Re Patent Application of:
HYLAND
Serial No. 10/806,936
Filing Date: MARCH 23, 2004

CONCLUSIONS

In view of the foregoing arguments, it is submitted that all of the claims are patentable over the prior art. Accordingly, the Board of Patent Appeals and Interferences is respectfully requested to reverse the earlier unfavorable decision by the Examiner.

Respectfully submitted,



JEREMY B. BERMAN, ESQ.
Reg. No. 60,582
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Appellant

In Re Patent Application of:

HYLAND

Serial No. 10/806,936

Filing Date: MARCH 23, 2004

APPENDIX A - CLAIMS ON APPEAL

FOR U.S. PATENT APPLICATION SERIAL NO. 10/806,936

1. (Previously Presented) A cryptographic device comprising:

 a cryptographic module and a communications module removably coupled thereto;

 said cryptographic module comprising a first housing and a first connector carried thereby, said first housing comprising a first body and a first extension extending outwardly therefrom;

 said communications module comprising a second housing and a second connector carried thereby and being removably mateable with said first connector of said cryptographic module, said second housing comprising a second body and a second extension extending outwardly therefrom;

 said first and second extensions being aligned in overlapping relation when said first and second connectors are mated together;

 said first connector carried by said first body adjacent said first extension and said second connector carried by said second extension.

2. (Canceled)

3. (Canceled)

4. (Original) The cryptographic device of Claim 2 wherein each of said first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide said cryptographic and communications modules together in

mating relation.

5. (Original) The cryptographic device of Claim 4 wherein said surface features define at least one slidable interlocking joint therebetween.

6. (Original) The cryptographic device of Claim 1 further comprising at least one fastener for removably fastening said cryptographic and communications modules together.

7. (Original) The cryptographic device of Claim 1 wherein said at least one fastener comprises at least one captive screw.

8. (Original) The cryptographic device of Claim 1 wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

9. (Original) The cryptographic device of Claim 1 wherein said communications module further comprises a network communications interface carried by said second housing and coupled to said second connector.

10. (Original) The cryptographic device of Claim 1 wherein said first and second connectors each comprise multi-pin electrical connectors.

11. (Original) The cryptographic device of Claim 1 further comprising at least one seal between said cryptographic module and said communications module.

12. (Previously Presented) A cryptographic device comprising:

a cryptographic module, a communications module removably coupled to said cryptographic module, and at least one fastener for removably fastening said cryptographic and communications modules together;

said cryptographic module comprising a first housing and a first connector carried thereby, said first housing comprising a first body and a first extension extending outwardly therefrom;

said communications module comprising a second housing and a second connector carried thereby, said second housing comprising a second body and a second extension extending outwardly therefrom;

said second connector being removably mateable with said first connector of said cryptographic module, and said first and second extensions being aligned in overlapping relation when said first and second connectors are mated together;

said first connector carried by said first body adjacent said first extension and said second connector carried by said second extension.

13. (Canceled)

14. (Original) The cryptographic device of Claim 12 wherein each of said first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide said cryptographic and communications modules together in mating relation.

In Re Patent Application of:
HYLAND
Serial No. 10/806,936
Filing Date: MARCH 23, 2004

15. (Original) The cryptographic device of Claim 14 wherein said surface features define at least one slidable interlocking joint therebetween.

16. (Original) The cryptographic device of Claim 12 wherein said at least one fastener comprises at least one captive screw.

17. (Original) The cryptographic device of Claim 12 wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media.

18. (Original) The cryptographic device of Claim 12 wherein said communications module further comprises a network communications interface carried by said second housing and coupled to said second connector.

19. (Original) The cryptographic device of Claim 12 wherein said first and second connectors each comprise multi-pin electrical connectors.

20. (Original) The cryptographic device of Claim 12 further comprising at least one seal between said cryptographic module and said communications module.

21. (Previously Presented) A communications method comprising:
coupling a cryptographic module to a network device, the cryptographic module comprising a first housing and a first connector carried thereby, the first housing comprising a first

body and a first extension extending outwardly therefrom;
providing a communications module comprising a second housing and a second connector carried thereby with the second connector of the communications module being removably mated with the first connector of the cryptographic module, the second housing comprising a second body and a second extension extending outwardly therefrom;
the first and second extensions aligned in overlapping relation when the first and second connections are mated together, the first connector carried by the first body adjacent the first extension and the second connector carried by the second extension; and
using the communications module to communicate with a network.

22. (Canceled)

23. (Canceled)

24. (Original) The method of Claim 22 wherein each of the first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide the cryptographic and communications modules together in mating relation.

25. (Original) The method of Claim 24 wherein the surface features define at least one slidable interlocking joint therebetween.

26. (Original) The method of Claim 21 further comprising removably fastening the cryptographic and communications modules together.

27. (Original) The method of Claim 21 further comprising positioning at least one seal between the cryptographic module and the communications module.

28. (Previously Presented) A communications system comprising:

a plurality of network devices coupled together to define a network, and a cryptographic device coupled to at least one of said network devices;

said cryptographic device comprising a cryptographic module coupled to said at least one network device, and a communications module removably coupled to said cryptographic module;

said cryptographic module comprising a first housing and a first connector carried thereby, said first housing comprising a first body and a first extension extending outwardly therefrom;

said communications module comprising a second housing and a second connector carried thereby and being removably mateable with said first connector of said cryptographic module, said second housing comprising a second body and a second extension extending outwardly therefrom;

said first and second extensions being aligned in overlapping relation when said first and second connectors are mated together;

said first connector carried by said first body adjacent said first extension and said second connector carried by said second extension.

29. (Canceled)

30. (Canceled)

31. (Original) The communications system of Claim 29 wherein each of said first and second extensions have surface features on opposing surfaces thereof to slidably engage and guide said cryptographic and communications modules together in mating relation.

32. (Original) The communications system of Claim 31 wherein said surface features define at least one slidable interlocking joint therebetween.

33. (Original) The communications system of Claim 28 further comprising at least one fastener for removably fastening said cryptographic and communications modules together.

34. (Original) The communications system of Claim 33 wherein said at least one fastener comprises at least one captive screw.

35. (Original) The communications system of Claim 28 wherein said cryptographic module further comprises:
a user network interface carried by said first housing;
and
a cryptographic processor carried by said first housing
and coupled to said user network interface and said first connector.

36. (Original) The communications system of Claim 28 wherein said communications module further comprises a network

In Re Patent Application of:
HYLAND
Serial No. 10/806,936
Filing Date: MARCH 23, 2004

communications interface carried by said second housing and coupled to said second connector.

37. (Original) The communications system of Claim 28 wherein said first and second connectors each comprise multi-pin electrical connectors.

38. (Original) The communications system of Claim 28 further comprising at least one seal between said cryptographic module and said communications module.

In Re Patent Application of:
HYLAND
Serial No. 10/806,936
Filing Date: MARCH 23, 2004

APPENDIX B - EVIDENCE APPENDIX
PURSUANT TO 37 C.F.R. § 41.37(c)(1)(ix)

None.

In Re Patent Application of:
HYLAND
Serial No. 10/806,936
Filing Date: MARCH 23, 2004

APPENDIX C - RELATED PROCEEDINGS APPENDIX
PURSUANT TO 37 C.F.R. § 41.37(c)(1)(x)

None.